UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN RE:

APPLICATION OF INTERNATIONAL MINERAL RESOURCES B.V. FOR AN ORDER TO TAKE DISCOVERY PURSUANT TO 28 U.S.C. § 1782

Applicant.

Case No. _____

DECLARATION OF JONATHAN D. COGAN

EXHIBIT G

EXHIBIT L

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: APPLICATION OF INTERNATIONAL MINERAL RESOURCES B.V. FOR AN ORDER TO TAKE DISCOVERY PURSUANT TO 28 U.S.C. § 1782 Applicant.	Case No. 1:14-MC-00340 (GK)

DECLARATION OF MELANIE MAUGERI

Pursuant to 28 U.S.C. § 1746, I, Melanie Maugeri, declare under penalty of perjury as follows:

1. I am a Digital Forensic Examiner at Stroz Friedberg, LLC ("Stroz Friedberg"). I submit this Declaration in support of International Mineral Resources B.V.'s ("IMR") Motion to Compel Production of Documents and Additional Day of Deposition and Motion for Expedited Consideration. Because this declaration is being submitted for a specific legal purpose, the information provided in the declaration does not include every fact that I know that may be pertinent to the matter nor does it describe every step of the forensic analysis undertaken to reach the findings described below.

2. I have been employed at Stroz Friedberg since 2011 and currently serve as a Digital Forensic Examiner in the company's San Francisco office. Stroz Friedberg is a consulting and technical services firm specializing in computer forensics; data breach and computer crime response; cyber investigations; and electronic data preservation, analysis and production. The firm has domestic offices in New York, Washington, DC, Los Angeles, San Francisco, Boston, Chicago, Minneapolis, Seattle, and Dallas, as well international offices in London, UK, Zurich, Switzerland, and Hong Kong. The firm's management and technical staff includes former Assistant United States Attorneys, former agents of the Federal Bureau of

Investigation, the U.S. Department of Defense, U.S. Air Force Office of Special Investigations, and other government agencies, as well as information security professionals.

3. I have been trained in the use of computer forensic tools and techniques, including forensic tool sets such as EnCase, Access Data's Forensic Toolkit, and Blacklight. I also have received training in the investigation and analysis of networked and stand-alone systems, including Microsoft Windows, Mac, and Linux operating systems. I have forensically acquired and analyzed thousands of items of digital media, including desktops, laptops, and server computers, external drives, and handheld devices. In addition, I have authored or assisted in the drafting of numerous expert reports on a variety of computer forensic matters, including metadata analysis, file deletion activity, the chronology of movement of electronic documents among different storage media, and the analysis of the authors and editors of key electronic documents. Attached as Exhibit A to this declaration is a true, correct, and current copy of my curriculum vitae, which sets forth in detail additional aspects of my qualifications, experience, and background.

4. Stroz Friedberg was retained by Kobre & Kim LLP ("Kobre & Kim") on behalf of IMR to preserve and examine a SanDisk USB thumb drive ("Thumb Drive") bearing the Serial Number 2006026692115C918C4A. At the request of Kobre & Kim, I subsequently performed a forensic examination of the embedded metadata of the files found on the Thumb Drive to determine, among other things, information concerning who had accessed the files contained on the device.

5. Metadata is information about a file's characteristics and properties and generally can be defined as "data about data." A file's metadata may be stored within the file itself, or stored externally to the file. The metadata available for a file depends on several factors, including the digital media on which the file was stored, the file system on the digital media, and the application or applications used to create, modify, and view the file. Metadata can refer to many characteristics or properties of a file including, in certain circumstances, who may have accessed the file. There are two distinct types of metadata, embedded metadata which is

typically found within electronic files and files system metadata which is tracked by the file system.

6. More specifically, the WriteAccess embedded metadata field of a Microsoft Excel Spreadsheet and the CurrentUser field of a Microsoft PowerPoint Presentation are typically populated with the application's registered user name when the file is opened, even if no changes are made to the content of the file.

7. By analyzing both the WriteAccess and CurrentUser embedded metadata fields, I found evidence indicating that certain files on the Thumb Drive had been accessed by a user identified as "RA."

8. By analyzing both the WriteAccess and CurrentUser embedded metadata fields, I found evidence indicating that certain files on the Thumb Drive had been accessed by a user identified as "Scott Horton."

9. I declare under penalty of perjury under the laws of the United States and the state of California that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 18th day of May 2015, at San Francisco, California.

STROZ FRIEDBERG, LLC

By: Melanie A. Maugeri

Melanie A. Maugeri